

1 **In the Claims**

2 Claims 1-3, 6, 13, 16, 20, 23-25, 28, and 32-33 are currently amended.

3 Claims 4-5, 14-15, 21-22, 26, and 29 are canceled.

4 Claims 1-3, 6-13, 16-20, 23-25, 27-28, and 30-33 are pending and are listed
5 below.

6

7 1. (Currently Amended) A processor-readable medium having a
8 tangible component and comprising processor-executable instructions configured
9 for:

10 receiving a binary signature at a server computing device;

11 receiving a security patch at the server computing device;

12 identifying, from the server computing device, a vulnerable binary file
13 located on a computerclient computing device based on the binary signature, the
14 client computing device being remote from the server computing device; and

15 updating, from the server computing device, the vulnerable binary file
16 located on the computerclient computing device with the security patch.

17

18 2. (Currently Amended) A processor-readable medium as recited in
19 claim 1, wherein the identifying a vulnerable binary file located on a
20 computerclient computing device includes comparing a bit pattern of the binary
21 signature against binary files located on the computerclient computing device, the
22 bit pattern associated with a security vulnerability.

23

24 3. (Currently Amended) A processor-readable medium as recited in
25 claim 1, wherein the updating the vulnerable binary file located on the

1 computerclient computing device includes installing the security patch on the
2 computerclient computing device from the server computing device.

3

4 4. (Canceled)

5

6 5. (Canceled)

7

8 6. (Currently Amended) A processor-readable medium as recited in
9 claim 1, wherein the computer is a client computer and the receiving includes
10 receiving the binary signature and the security patch from a distribution server
11 configured to distribute to the client computercomputing device, binary signatures
12 that identify vulnerable files and security patches configured to fix the vulnerable
13 files.

14

15 7. (Original) A server comprising the processor-readable medium as
16 recited in claim 1.

17

18 8. (Previously Presented) A processor-readable medium having a
19 tangible component and comprising processor-executable instructions configured
20 for:

21 receiving a binary signature that identifies a security vulnerability in a
22 binary file;

23 receiving a security patch configured to fix the security vulnerability in the
24 binary file; and

1 distributing the binary signature and the security patch to a plurality of
2 servers.
3

4 9. (Original) A processor-readable medium as recited in claim 8,
5 wherein the distributing includes:

6 sending a notice to each of the plurality of servers regarding the security
7 vulnerability and the available patch;

8 receiving a request to send the binary signature and the security patch; and

9 sending the binary signature and the security patch in response to the
10 request.

11

12 10. (Original) A distribution server comprising the processor-readable
13 medium as recited in claim 8.

14

15 11. (Previously Presented) A processor-readable medium having a
16 tangible component and comprising processor-executable instructions configured
17 for:

18 receiving a binary signature from a server;

19 searching for the binary signature in binary files located on a client
20 computer;

21 sending a request from the client computer to the server for a security patch
22 if a binary file is found that includes the binary signature;

23 receiving the security patch from the server; and

24 updating on the client computer the binary file with the security patch.

1 **12.** (Original) A client computer comprising the processor-readable
2 medium as recited in claim 11.

3

4 **13.** (Currently Amended) A method comprising:
5 receiving a binary signature from a server and at a client computer;
6 searching on the client computer for a vulnerable file based on the binary
7 signature;

8 if a vulnerable file is found on the client computer, requesting a security
9 patch from the server;[[and]]

10 receiving the security patch from the server and at the client computer in
11 response to the request for the security patch from the client computer; and
12 fixing the vulnerable file with the security patch received from the server.

13

14 **14.** (Canceled)

15

16 **15.** (Canceled)

17

18 **16.** (Currently Amended) A method as recited in claim 13, wherein the
19 fixing includes installing the security patch on a computerthe client computer.

20

21 **17.** (Original) A method as recited in claim 13, wherein the searching
22 includes comparing the binary signature to binary information on a storage
23 medium of a computerthe client computer.

1 **18.** (Previously Presented) A method as recited in claim 17, wherein the
2 binary information is selected from a group comprising:

- 3 an operating system;
4 an application program file; and
5 a data file.

6

7 **19.** (Previously Presented) A method as recited in claim 17, wherein the
8 storage medium is selected from a group comprising:

- 9 a hard disk;
10 a magnetic floppy disk;
11 an optical disk;
12 a flash memory card;
13 an electrically erasable programmable read-only memory; and
14 network-attached storage.

15

16 **20.** (Currently Amended) A method comprising:

17 receiving, at a scan/patch server, a binary signature and a security patch
18 from a distribution server;
19 searching, by the scan/patch server, on a client computer for a vulnerable
20 file associated with the binary signature; and
21 if a vulnerable file is found, fixing, by the scan/patch server, the vulnerable
22 file on the client computer with the security patch.

23

24 **21.** (Canceled)

25

1 **22.** (Canceled)

2

3 **23.** (Currently Amended) A computer comprising:

4 means for receiving, at a client computer, a binary signature from a server;

5 means for searching for a vulnerable file located on the client computer

6 based on the binary signature;

7 means for requesting, by the client computer, a security patch from the

8 server if a vulnerable file is found on the client computer;[[and]]

9 means for receiving the security patch from the server at the client

10 computer responsive to the request for the security patch; and

11 means for fixing the vulnerable file with the security patch received from

12 the server.

13

14 **24.** (Currently Amended) A server comprising:

15 means for receiving, at a scan/patch server, a binary signature and a

16 security patch from a distribution server;

17 means for scanning, from the scan/patch server, a client computer for a

18 vulnerable file associated with the binary signature; and

19 means for fixing, from the scan/patch server, the vulnerable file on the

20 client computer with the security patch if a vulnerable file is found on the client

21 computer.

22

23 **25.** (Currently Amended) A computer having a tangible component and

24 comprising:

25 binary information;

1 a storage medium configured to retain the binary information;
2 a scan module configured to receive a binary signature from a server and
3 scan the binary information on the computer for the binary signature; and
4 a patch module configured to request a security patch from a server and
5 install the security patch from the server if the binary signature is found in the
6 binary information on the computer.

7

8 **26.** (Canceled)

9

10 **27.** (Previously Presented) A computer as recited in claim 25, wherein
11 the binary information is selected from a group comprising:
12 an operating system;
13 an application program file; and
14 a data file.

15

16 **28.** (Currently Amended) A computer having a tangible component and
17 comprising:

18 binary files;
19 a storage medium configured to retain the binary files;
20 a binary signature; and
21 a security patch module configured to receive the binary signature from a
22 server and to scan the binary files on the computer in search of the binary
23 signature[[.]];
24 a binary file that includes the binary signature; and
25 a security patch;

1 wherein the security patch module is further configured to request the
2 security patch from the server upon locating the binary signature within the binary
3 file, and to apply the security patch to the binary file that includes the binary
4 signature.

5
6 **29.** (Canceled)

7
8 **30.** (Previously Presented) A distribution server having a tangible
9 component and comprising:

10 a database; and

11 a distribution module configured to receive a binary signature and a
12 security patch, store the binary signature and the security patch in the database,
13 and distribute the binary signature and the security patch to a plurality of servers.

14
15 **31.** (Original) A distribution server as recited in claim 30, wherein the
16 distribution module is further configured to receive a request from a server for the
17 binary signature and the security patch and to distribute the binary signature and
18 the security patch to the server in response to the request.

19
20 **32.** (Currently Amended) A server having a tangible component and
21 comprising:

22 a binary signature associated with a security vulnerability in a binary file;

23 a security patch configured to fix the security vulnerability in the binary
24 file;[[and]]

1 a database embodied as a storage medium and configured to store the
2 binary signature and the security patch;

3 a scan module configured to scan, from the server, binary files on a client
4 computer for the binary signature and to update, from the server, the binary file on
5 the client computer with the security patch if the binary signature is found,
6 wherein the client computer is remote from the server.

7

8 **33.** (Currently Amended) A server as recited in claim 32, further
9 comprising:

10 a database;

11 wherein the scan module is further configured to receive the binary
12 signature and the security patch from a distribution server and to store the binary
13 signature and the security patch in the database.